

**Kirstin Barrie**

**ID# 300022986**

**Balancing Security and  
Accountability: SIS Legislation and  
Recent Amendments.**

Submitted for the LLB (Hons) Degree  
at Victoria University of Wellington

1 September 1999

e  
AS741  
VUW  
A66  
B275  
1999

B275  
BARRIE, K.  
Balancing security and accountability.

VICTORIA  
UNIVERSITY OF  
WELLINGTON

*Te Whare Wananga  
o te Upoko o te Ika a Maui*



LIBRARY



# TABLE OF CONTENTS

Table of Cases .....	i
I Introduction .....	1
II Background .....	2
A Preceding Acts .....	2
B Issue of Interception Warrants .....	3
C Accountability Provisions .....	3
III <i>Choudry v Attorney-General</i> .....	4
A Facts .....	4
B Interception Warrant Question - the High Court Decision .....	5
C Public Interest Immunity: the High Court Decision .....	6
D Interception Warrant Question - the Court of Appeal Decision .....	6
E Public Interest Immunity: the Court of Appeal Decision .....	7
F Was the Court of Appeal Correct? .....	8
IV New Zealand Security Intelligence Service Amendment Bill 1998 .....	8
A Original Bill .....	8
B Changes Made by the Committee .....	9
C Submissions Relating to the Above Changes .....	10
V New Zealand Security Intelligence Service Amendment Bill (No 2) 1999 .....	11
A The Second Bill .....	11
B Submissions Addressed in the Second Bill .....	12
VI Other Issues Arising from the Bill .....	13
A No Need for a Secret Service .....	13
B No Accountability .....	14
C Search and Seizure Already has Widespread Legislative Provision .....	15
D Did the 1977 Parliament Intend the SIS to have the Power .....	16
E Breach of the International Covenant on Civil and Political Rights .....	16
F Not Many Warrants .....	17
G Lack of Competency Examples .....	17
H Is it Possible for the SIS to Act Properly Without the Power .....	17
I Bill of Rights Act 1990, Section 21 .....	18
VII Conclusion .....	18
Bibliography .....	20



**TABLE OF CASES**

<i>Choudry v Attorney-General</i> (19 August 1998) unreported, High Court, Christchurch Registry, CP 15/98 .....	5, 6
<i>Choudry v Attorney-General</i> (9 December 1998) unreported, Court of Appeal, CA 217/98 .....	6
<i>Choudry v Attorney-General</i> (6 July 1999) unreported, Court of Appeal, CA 217/99.....	8
<i>Corbett v Social Security Commission</i> [1962] NZLR 878 (CA) .....	7
<i>Dulcie Holdings Ltd v New Zealand Customs Service</i> [1997] DCR 1077 (DC) .....	15
<i>Entick v Carrington</i> [1765] 95 ER 807 (KB) .....	5
<i>Haj-Ismael v Maddigan</i> (1982) 45 ALR 379 (FCA) .....	6
<i>Liversidge v Anderson</i> [1942] AC 206 (HL) .....	15
<i>Meates v Attorney-General (Customs Department)</i> [1981] 2 NZLR 335 (HL) .....	15
<i>Morris v Beardmore</i> [1981] AC 446 (HL) .....	5
<i>Police v Anderson</i> [1977] NZLR 233 (CA) .....	15
<i>R v Laugalis</i> (1993) 1 HRNZ 466 (CA) .....	18



## I INTRODUCTION

One of the fundamental tenets of a democratic state is public accountability for all branches of government. This presupposes that the public has a right to be informed about what the government is doing, and can ultimately sanction or penalise these actions on election date. A covert intelligence agency, then, would appear to be a thorn in the side of a democratic state. Reconciling the two notions of accountability and security of state has long been something with which New Zealand, and other democratic states, have struggled.

The New Zealand Security Intelligence Service (SIS) was brought into existence on 28 November 1956 by an Order in Council.<sup>1</sup> From this time until the New Zealand Security Intelligence Service Act 1969 (the principal Act) was passed the very existence of the SIS, not to mention its role and functions within society, were hidden in the shadowy realms of Crown prerogative. In 1969 Parliament made a conscious decision to bring the SIS, in part at least, out into the open. Although the principal Act basically preserved the status quo it was widely felt that it was "...desirable that [the SIS] should be subject to the specific provisions of the law."<sup>2</sup> Given that New Zealand is a rule of law state, allowing none to be above the law, this stance is hardly surprising; even less so when it is considered that the operation of such a service necessarily involves infringement upon individuals' rights and liberties.

As one would expect, a central issue up for debate when the principal Act was passed (and every time the SIS has come under public scrutiny since then) was whether it is possible to reconcile the secretive nature of a security agency with the principles of a democracy. Prima facie there appears to be a direct conflict - "...[o]n the one hand the State claims to guarantee freedoms, and on the other monitors the activities of people who exercise them."<sup>3</sup> Most people seem willing to accept some friction on the basis that the continued existence of our democratic society needs to be ensured by protecting the state from genuine subversive threats. Proponents of the SIS describe its main function as protecting democracy from the knife at its throat. It needs to be remembered, however, that without the balancing feature of accountability the SIS itself could become the knife at our democracy's throat.

Although this struggle is by no means novel, recent developments in this area provide an unique illustration of how the balancing system should work now that the SIS is a statutory body - starting with the 1996 amendment to the principal Act and the *Choudry* case, and culminating in the 1998/1999 amendments.

<sup>1</sup> This paper is concerned only with the SIS, for a full discussion of the Government Communications Security Bureau (GCSB) see Nicky Hagar *Secret Power: New Zealand's Role in the International Spy Network* (Craig Potton Publishing, Nelson, 1996).

<sup>2</sup> New Zealand Council for Civil Liberties, Report on the New Zealand Security Service Intelligence Act 1969, (Wellington, 1971), 4.

<sup>3</sup> G. Crowder "The Security Intelligence Service Amendment Act 1977 and the State Power to Intercept Communications" (1977/78) 9 VUWLR 145, 152.



## II BACKGROUND

### A *Preceding Acts*

Before considering the recent events it is important to have a grasp of the initial statutory framework; Parliament's first attempts to grapple with reconciling accountability and security through legislation.

The principal Act was enacted in 1969 to "...make better provision for the New Zealand Security Intelligence Service."<sup>4</sup> It provided for the service to obtain, correlate and evaluate intelligence, to advise Ministers of the Crown in respect of matters relevant to security and to co-operate with authorities in New Zealand and overseas.<sup>5</sup>

The New Zealand Security Intelligence Service Amendment Act 1977 was passed subsequent to a report by the then Chief Ombudsman, the late Sir Guy Powles, which recommended that the SIS be given powers to intercept and seize any communication that was not otherwise lawfully obtainable, under a Ministerial warrant.<sup>6</sup> The Amendment Act also provided that no civil or criminal proceedings would lie against those doing anything "...necessarily involved in .. the interception."<sup>7</sup> It seems reasonably clear, with hindsight, that although the SIS had been a statutory body for eight years at this time, with all its powers supposedly set out for all to see, there was still a reluctance to actually admit what they were doing, that is to explicitly state that individual's homes were being broken into when it was considered necessary.

In 1996 the principal Act was again amended, setting in motion the chain of events of interest here. The amendment of major concern was the altering of the definition of security from

the protection of New Zealand from acts of espionage, sabotage, terrorism and subversion, whether or not it is directed from or intended to be committed within New Zealand.<sup>8</sup>

to include

the making of a contribution to New Zealand's international well-being or economic well-being.<sup>9</sup>

A chorus of objectors strongly argued that this inclusion made the definition of security too wide and subjective; also that it was open to abuse and could be used by politicians to further their own agenda by classifying activists with views contrary to their own as

<sup>4</sup> New Zealand Security Intelligence Service Act 1969, long title. [The principal Act]

<sup>5</sup> The principal Act, above n4, s4.

<sup>6</sup> New Zealand Security Intelligence Service Amendment Act 1977, s4 (inserting s4A into the principal Act) [1977 Amendment].

<sup>7</sup> 1977 Amendment, above n6, s4(6) (inserting s4A(6) into the principal Act).

<sup>8</sup> The principal Act, above n4, s2 "Security."

<sup>9</sup> New Zealand Security Intelligence Service Amendment Act 1996, s2(3) [1996 Amendment].



being threats to New Zealand's economic well-being, thereby subjecting them to surveillance. Those that made submissions to parliament to that effect were told by Committee members that they were paranoid and naive. Ironically these concerns seemed to be vindicated only two weeks after the legislation was passed when the SIS broke into the home of Mr Choudry, a well known critic of government policies and practices. It remains to be seen exactly what sort of threat to New Zealand Mr Choudry was.<sup>10</sup> The Amendment Act also added to section 4 of the principal Act, the provision that the Act would not limit the right of people to engage in lawful dissent and that the exercise of this right would not be enough on its own to justify surveillance by the SIS.<sup>11</sup> However it is unclear how effective this provision is in practice given that it is almost impossible to tell if the SIS are abiding by it or not.

### ***B Issue of Interception Warrants***

The Ministerial interception warrants provided for by the 1977 Amendment Act, under section 4A(1) of the principal Act, may be issued provided the Minister is satisfied that

- (a) The interception or seizure is necessary either
  - (i) For the detection of activities prejudicial to security; or
  - (ii) For the purpose of gathering foreign intelligence .. essential to security; and
- (b) The value of the information sought .. is such as to justify the particular interception or seizure; and
- (c) The information is not likely to be obtained by any other means; and
- (d) The information is not privileged..

It is therefore up to the Minister to balance the competing interests of security and an individual's right to privacy and freedom from interference.

Section 4A(2) provides that any warrant shall specify the type of communication to be intercepted as well as the identity of the persons whose communications are sought to be intercepted (known as a 'person warrant') or, if their identity is not known, the place where the communications may be intercepted or seized (known as a 'place warrant').

### ***C Accountability Provisions***

The principal Act expressly confronts the issue of accountability, despite the need for secrecy, providing a number of controls on the issue and use of interception warrants.<sup>12</sup> The application to the Minister for an interception warrant to be issued can only be made by the Director of Security, or his/her Deputy, and must be made in writing with the accompanying facts or evidence sworn on oath. The commencing of the process is therefore claimed to be non-political with an upward, as opposed to downward, moving power.<sup>13</sup> The Minister is answerable to Parliament and must annually review all warrants

<sup>10</sup> GATT Watchdog "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998.", 1.

<sup>11</sup> 1996 Amendment, above n9, s4(3).

<sup>12</sup> For a discussion of Australian, Canadian and United Kingdom accountability mechanisms see Lawrence Lustgarten "Accountability of Security Services in Western Democracies" (1992) 45 Current Legal Prob 146.

<sup>13</sup> Crowder, above n3, 156.



issued and lay a report before Parliament relating to the number of warrants issued in the preceding year.<sup>14</sup>

Also in 1996 two associated pieces of legislation were passed, partly to offset the concurrent increase of the SIS's powers through the widening of the definition of security, and therefore the ambit of responsibility. The Intelligence and Security Committee Act created the five member Committee in charge of overseeing policy issues relevant to the SIS. The Inspector-General of Intelligence and Security Act (IGISA) was enacted to increase the oversight and review of intelligence and security agencies. The Inspector-General's functions are to<sup>15</sup>

- inquire into any matter that relates to intelligence and security agencies compliance with the law - section 11(1)(a)
- inquire into any complaint by a New Zealand person that that person has been adversely affected by .. an intelligence and security agency - section 11(1)(b)
- inquire into any matter where a New Zealand person may have been adversely affected, and inquire into the propriety of particular activities - section 11(1)(c)
- review the effectiveness and appropriateness of the procedures adopted by the SIS to ensure compliance with section 4A and section 4B of the principal Act - section 11(1)(d)
- prepare and submit to the Minister programmes for general oversight and review of each intelligence and security agency - section 11(1)(e) and (f).

The Inspector-General, however, is not allowed to inquire into any action taken by the Minister (section 11(2)(3)) nor "...into any matter that is operationally sensitive, including any matter that relates to intelligence collection and production methods or sources of information." (section 11(2)(4))

The Inspector-General has powers to recommend to the Minister redress for the complainant, including remedies that involve payment of compensation - section 11(6). However, these powers were of no use to Mr Choudry when the SIS broke into his home soon after the 1996 Amendment, as the Inspector-General's report simply stated that the SIS actions were not illegal, and that Mr Choudry should not, therefore, receive any form of redress.

### **III CHOUDRY V ATTORNEY-GENERAL**

The second stage of events was the unusual chance presented to the courts to examine the 1977 Amendment, 19 years after the event, and to undertake its own balancing exercise of security interests and accountability.

<sup>14</sup> 1977 Amendment, above n6, s4 (inserting s4A(5) into the principal Act ).

<sup>15</sup> As summarised by Sir Geoffrey Palmer "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998.", 3-4.



### **A Facts**

The plaintiff, Abdul Aziz Choudry, is a well known political activist and member of a group known as GATT Watchdog. A GATT Watchdog Conference on Free Trade was being held in opposition to the APEC Trade Ministers meeting which was to take place during the week beginning 15 July 1996.

On 13 July 1996 a colleague of the plaintiff's, Dr Small, disturbed two men rifling through papers in the plaintiff's home. In response to this unauthorised entry of his home the plaintiff issued proceedings claiming \$150 000 damages for trespass or, alternatively, for a breach of his rights to protection from unreasonable search and seizure, under New Zealand Bill of Rights Act 1990 (BORA), section 21.

The Attorney-General pleaded as defence that the entry was lawful since it was done pursuant to an interception warrant issued under section 4A(1) of the principal Act. The warrant was a person warrant, not a place warrant, but it was unclear whether the plaintiff was the sole subject of the warrant or just one of a number of persons identified in it as all relevant provisions were deleted from the version of the warrant before the Court.

There were two main issues to be decided

- (1) whether the interception warrant authorised entry into the plaintiff's home; and
- (2) whether public interest immunity could apply to all the documents for which it was claimed, in relation to a better discovery application.

### **B Interception Warrant Question: the High Court Decision**

Counsel formulated the issue by drawing a distinction between entry onto premises and breaking and entering private dwellings. Justice Panckhurst saw no material distinction between the two and addressed them as one. However he accepted the distinction between person and place warrants. The plaintiff argued that section 4A allows the Minister to issue an interception warrant allowing for "the interception or seizure of any communication," and neither expressly nor impliedly authorises entry onto premises, let alone breaking and entering. Counsel for the SIS argued that by necessary implication an interception warrant authorises entry onto private property, and breaking and entering, to intercept or seize communications.

A useful starting point is the common law. Justice Panckhurst quoted several cases, including Lord Scarman's speech in *Morris v Beardmore*<sup>16</sup>, which makes reference to the famous *Entick v Carrington*<sup>17</sup> case, and concluded that "...only if Parliament had spoken clearly should a power of entry be found to exist."<sup>18</sup> However, the judge continued, this is not to say that legislative intention cannot be imputed from the words of the legislation,

<sup>16</sup> [1981] AC 446, 464 (HL).

<sup>17</sup> (1765) 95 ER 807 (KB).

<sup>18</sup> *Choudry v Attorney-General* (19 August 1998) unreported, High Court, Christchurch Registry, CP 15/98, 11 [Choudry HC].



so long as the implication is "...necessary in the sense that otherwise the very purpose and effect of the section would be frustrated."<sup>19</sup>

Justice Panckhurst concluded that an interception warrant issued under section 4A of the principal Act authorises covert entry onto premises in order to seize or intercept communications, for three reasons;

(1) the context of the section. The Act is intended to make better provision for the SIS so that it can act to protect New Zealand from "activities which may strike at the core of the nation's well-being."<sup>20</sup>

(2) the concept of interception is defined by an inclusive definition in section 2 of the principal Act. How interception and seizure are carried out is left unspecified by Parliament. This must have been deliberate and therefore, in the judge's view, carries with it the necessary implication that covert entry was contemplated.

(3) the principal Act allows for both interception and seizure. Although interception is possible without entry onto property, the additional power to seize, especially in the context of written documents, indicates again that covert entry must have been envisaged.

This conclusion applies to both person and place warrants since "...ownership or occupation of premises by a person identified in the warrant cannot be the limiting criteria."<sup>21</sup> In the learned Judge's opinion limiting factors are given in section 4A(6) of the principal Act which grants immunity for "...reasonable action necessarily involved in making .. the interception or seizure.." (emphasis added).

#### **C Public Interest Immunity: the High Court Decision**

Verified lists of documents were exchanged between the parties and in relation to about 70 of the documents objection was raised to their production on the grounds of public interest. Justice Panckhurst considered that it would not be appropriate to uphold the Prime Minister's certificate advising against disclosure without inspection of the documents. He came to this conclusion because of two main considerations. The first was the relevance of most, if not all, of the documents. The sole defence to the trespass and unreasonableness claims was lawful authority, so documents relating to the ambit and implementation of the warrant will be highly relevant in deciding these issues. Secondly, no detailed reasons were given to support the Prime Minister's claim that producing the documents would be prejudicial to security.<sup>22</sup> Also, the Act provides that the right of lawful dissent should not be limited and the plaintiff's descriptions of the nature of his activities at the time as solely political remain unchallenged.

#### **D Interception Warrant Question: the Court of Appeal Decision**

The Court of Appeal unanimously reversed Justice Panckhurst's finding that the interception warrant authorised entry into the plaintiff's home. They found that the focus

<sup>19</sup> Choudry HC, above n18, 12

<sup>20</sup> Choudry HC, above n18, 19.

<sup>21</sup> Choudry HC, above n18, 21.

<sup>22</sup> Compare with *Haj-Ismail v Maddigan* (1982) 45 ALR 379 (FCA).



of section 4A is the interception of communications which "...refers to the action of gaining access to information which is being passed from .. source to intended destination."<sup>23</sup> The section allows for interception of what is being passed and, although the method of such interception or seizure is left open, "...in the absence of clear authorisation it does not allow for the commission of further crimes or torts."<sup>24</sup>

There is nothing in the statutory scheme or language to suggest that interception warrants were intended to grant the SIS powers to enter onto private property without the owner's consent. Also relevant is that statutory provisions affecting bodies equivalent to the SIS in Australia, Canada and the United Kingdom all make express provision for warrants to authorise entry onto private property.<sup>25</sup> These statutes recognise that at common law any invasion onto private property is a trespass and it is a fundamental constitutional consideration that any erosion of common law protections should be set out in the clearest of terms. Therefore the power of entry, or of breaking and entering, onto private premises is not conferred by section 4A(1).

### *E Public Interest Immunity: the Court of Appeal Decision*

The Court of Appeal upheld the High Court decision that the Court should review the documents in question before deciding whether to uphold the Prime Minister's certificate. They recognised that while New Zealand courts pay deference to a certificate by a Minister that production of certain documents will be contrary to the public interest, they are not bound by it.<sup>26</sup> Most judicial statements about deferring to executive decisions have been made in the context of a narrow definition of the concept of national security, as opposed to the wide definition given in the principal Act. Also there has been a move in recent times to a more open government in New Zealand.

The Prime Minister's certificate claims immunity for a wide range of documents with only very vague reasons why the security of New Zealand would be affected. It is therefore unclear which aspect of security is involved, and so impossible to determine where the balance lies between public interest in keeping the documents confidential and public interest in effective administration of justice. Balancing these interests is a judicial function, not a Ministerial one, and the Court needs to be fully informed in order to carry out that exercise. The Court will only require inspection of the documents if the Prime

<sup>23</sup> *Choudry v Attorney-General* (9 December 1998) unreported, Court of Appeal, CA217/98, 15 [Choudry CA].

<sup>24</sup> *Choudry* CA, above n23, 15.

<sup>25</sup> See Australian Security Intelligence Organisation Act 1979, s25; Canadian Security Intelligence Act 1984, s21; United Kingdom Interception of Communications Act 1985, s3; Security Services Act 1989, s3 [deals with MI5 - the internal security body]; Intelligence Services Act 1994, s5 [deals with MI6 and GCHQ - the international security bodies]. For a discussion on these Acts and the Services they govern see Australia - H.P Lee, "The Australian Security Intelligence Organisation - New Mechanisms for Accountability" (1989) 38 ICLQ 890. Canada - L.L.J Edwards "The Canadian Security Intelligence Act 1984 - a Canadian Appraisal" (1985) 5 Oxford J Leg Studies 143. United Kingdom - Ian J Lloyd "The Interception of Communications Act 1985" (1986) 49 MLR 86; Ian Leigh and Laurence Lustgarten, "The Security Services Act 1989" (1989) 52 MLR 801; Philip Leach, "The Security Service Bill" (1996) 146 New L J 224; John Wadham, "The Intelligence Services Act 1994" (1994) 57 MLR 916.

<sup>26</sup> *Corbett v Social Security Commission* [1962] NZLR 878 (CA).



Minister does not file an amended certificate or if the amended certificate still leaves the Court in doubt as to the security interests to be balanced.

On 6 July 1999 the Court of Appeal considered the Prime Minister's amended certificate and held by a four to one majority that it should be upheld, and the relevant documents not produced. Although the certificate was not as particularised as the Court had suggested (that is it did not provide details on which aspect of security was involved on a document by document basis) it was much more detailed than the first. The Court then seemed to backtrack from their last decision on the matter by saying that the judiciary does not have the skills or knowledge to say that the Prime Minister's view is not correct. In his dissenting judgment, Justice Thomas stressed that the issue was whether the documents should be shown to the Court, not whether they should be made public. Also important was the fact that, in his opinion, the only way the SIS can be held accountable is through the courts, since it cannot be held truly accountable through Parliament due to national security concerns. In addition he restated the court's previous position that balancing public interests is a judicial function, and he seemed unable to reconcile the majority's position that the court could not do so competently, with placing trust in the Prime Minister to be able to do so.<sup>27</sup>

Mr Choudry is still planning on taking the SIS back to the High Court in relation to his damages claim for the break in.<sup>28</sup>

#### *F Was the Court of Appeal Correct?*

The issue of concern here is whether interception warrants issued under the principal Act authorised entry onto private property. It is clear that the Court of Appeal's approach is more black letter than the court below and, in this context, also more constitutionally correct. It was common ground between both courts that the power of entry onto private property should only be found if Parliament had clearly provided for it. The divergence arose as to the question of whether Parliament had so clearly provided. Although the High Court's reasons are well presented and quite compelling, the Court of Appeal's position of refusing to import a meaning not immediately clear into the words of a statute that infringes upon individual rights must be more correct. The fundamental principle of express authorisation for an invasion of rights, such as covert entry, must have been known by Parliament and so the absence of any express provision is a clear indication of Parliament's intent. Also, although the High Court's interpretation can logically be implied from the words in the section, it is going too far to say that it is a necessary implication in the sense that the section would have no effect if it was not interpreted in that manner.

Even if, contrary to the above argument, it was Parliament's intention to confer such a power, it is not the court's role to fix or patch up deficient legislation. It is for Parliament to clarify the position when it is insufficiently stated especially where, as in the present case, individual liberties are being infringed - which is exactly what Parliament did.

<sup>27</sup> *Choudry v Attorney-General* (6 July 1999) unreported, Court of Appeal, CA 217/99.

<sup>28</sup> Court of Appeal Rules in Favour of SIS" *Salient*, Wellington, New Zealand, 12 July 1999, 9.



#### **IV NEW ZEALAND SECURITY INTELLIGENCE SERVICE AMENDMENT BILL 1998**

##### **A Original Bill**

The New Zealand Security Intelligence Service Amendment Bill 1998 (the Bill) was introduced into Parliament on 16 December 1998 in response to the Court of Appeal's decision in *Choudry v Attorney-General* holding that there was no power of entry into private premises pursuant to an interception warrant. The purpose of the Bill is to confer express powers to enter property to install or remove devices/equipment or to remove material.<sup>29</sup> There is some debate, not to be covered in depth here, as to whether the Bill confers new powers on the SIS or whether it just confirms powers they have in reality had since the 1977 amendment.

Clause 3 of the Bill is the most important because it contains the provisions relating to interception warrants. It 'clarifies' that interception and seizure relate not only to communications but also to documents or "things". Clause 3(4) repeals section 4A(2)(b) of the principal Act and replaces it with a distinction between warrants for interception of communications and those for seizure of documents or things. So new paragraph (b) provides that a warrant should state the name of the person whose communications are to be intercepted, or the place where those communications are if the person's identity is not known. Paragraph (ba) then provides that if documents or things are to be seized the warrant should state the place where the documents or things are likely to be.

Clause 3(5) enacts subsections 3A to 3E, to be inserted after section 4A(3). Subsections 3B and 3C give express powers to enter any place specified in the warrant or any place where the person whose communications are to be intercepted is or is likely to be (subsection 3B) or, for a warrant to seize documents or things, any place specified in the warrant (subsection 3C).

The distinction between interception warrants for intercepting communications and those for seizing documents or things is important for in subsections 3D and 3E (also enacted by Clause 3(5)) different powers are conferred depending on whether the officer is acting pursuant to powers under subsection 3B or 3C.

##### **B Changes Made by the Committee**

The Committee made three changes designed to minimise the impact of interception warrants on third parties. Firstly, they qualified "any place" in subsection 3B so that under a warrant to intercept communications an officer can enter

- (a) any place specified in the warrant; or
- (b) any place owned/occupied by the person whose communications are to be intercepted; or
- (c) any place that person is likely to be, only with prior approval of the Director

Also, the Director must advise the Minister without delay of any approval given under

<sup>29</sup> New Zealand Security Intelligence Service Amendment Bill 1998, no 259-1, i (the commentary) [1998 Bill].



section 4A(3B)(c) and provides that everyone acting pursuant to an interception warrant must take all reasonable steps "...to minimise the likelihood of intercepting or seizing communications that are not relevant to [the person named in the warrant]"<sup>30</sup>

The word "thing" was removed and replaced it with "device or equipment" throughout clauses 3 and 4, that is in relation to the issue of interception warrants and the removal of things after the warrant ceases to be in force. However it is retained in new section 4A(3E) (powers while acting under a warrant to seize documents or things) when referring to being able to access any document or thing.

Lastly, clause 4 was amended, section 4AB(2)(ab) of the principal Act, to provide that all warrants shall specify a time period of validity not exceeding 12 months, with a right to reapply after expiry.

### *C Submissions Relating to the Above Changes*

#### *1. No time limit*

Providing, as the principal Act currently does, that interception warrants shall be "...valid for the time specified therein"<sup>31</sup> is quite a departure from police warrants issued under section 198 of the Summary Proceedings Act, which allows search warrants to exist for only 1 month. The power to enter houses can be open to abuse without checks and balances, one of which is to provide a finite term for warrants.<sup>32</sup> Another problem with having warrants valid for as long as each individual one states is that the information that was relied upon in order to issue that warrant may be 'stale' and out of date by the time it is acted upon. Rights of privacy should not be invaded on the basis of information that may no longer be correct. For example, in the *Choudry* case the warrant was 10 months old - issued 5 September 1995 and acted upon on 13 July 1996. It is argued that both the warrant and the information on which it was based were, by that stage, out of date.<sup>33</sup>

If this argument is accepted that 10 months is too long for a warrant to be in force, then the Committee's provision calling for all warrants to be in force for less than 12 months is a cosmetic change not really addressing the heart of the issue. Interestingly the Powles Report, which was the impetus for the 1977 Amendment Act, recommended that any warrant to intercept should have a maximum period of validity of ninety days.<sup>34</sup>

#### *2. "Any place" under a person warrant*

Allowing the SIS to enter any place where the person whose communications are to be intercepted is or is likely to be is a very extensive provision. All that would be required to search any individual's home would be a belief that the person named in the warrant may be at that place at any time. This would allow the SIS to break into the homes of

<sup>30</sup> 1998 Bill, above n29, cl 4A (inserting s4BA in the principal Act).

<sup>31</sup> The principal Act, above n4, s4A(2)(d).

<sup>32</sup> Dunedin Community Law Centre "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998.", 2.

<sup>33</sup> Auckland Council for Civil Liberties "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998.", 4.

<sup>34</sup> Report by Chief Ombudsman Security Intelligence Service (Wellington, 1976), 60.



completely innocent third parties who are not the subject of a warrant, which is an unacceptable extension of the warrant's scope.<sup>35</sup> Theoretically the amended requirement of obtaining the prior approval of the Director before exercising the statutory power should provide against unreasonable extensions of a warrant, but this safeguard is weakened by the fact that the Director is not completely removed from the situation, calling into question his/her impartiality when deciding what is reasonable and necessary.

3. *"Thing"*

The term "thing" is so general and unregulated that it could apply to anything whatsoever. Parliament needed to provide a "...more explicit definition of the types of devices and articles which [it] has in mind."<sup>36</sup> Allowing the SIS to install or remove any "thing" could point towards a very ominous conclusion as to just what exactly the SIS want to install or remove.<sup>37</sup>

**V NEW ZEALAND SECURITY INTELLIGENCE SERVICE AMENDMENT BILL (No 2) 1999**

**A The Second Bill**

The New Zealand Security Intelligence Service Amendment Bill (No 2) 1999 (the second Bill) was introduced to deal with other concerns raised by submissions to the first Bill. The second Bill is designed to provide greater certainty as to when SIS powers may be exercised and to provide safeguards against potential abuse.<sup>38</sup>

The second Bill divides interception warrants into two categories;

(1) foreign interception warrants: interception warrants not aimed at a New Zealand citizen or resident. They will continue to be issued by the Minister in charge of the SIS; and

(2) domestic interception warrants: all other interception warrants. They will be issued if both the Minister in charge of the SIS and the Commissioner of Security Warrants (the Commissioner) are satisfied that the conditions in the Act are met.

The Commissioner's position is enacted by clause 6 of the second Bill, inserting section 5A after section 5 in the principal Act. The Commissioner must have held office as a High Court judge (section 5A(3)) and is appointed for a term of three years, though s/he may be reappointed (section 5B(1)). This provides another example of Parliament attempts to maintain a balance between security and accountability. Another perceived increase in SIS powers calls for a further increase in accountability provisions - just as when the Inspector-General's role was created.

<sup>35</sup> Auckland Council for Civil Liberties, above n33, 5.

<sup>36</sup> Association of University of New Zealand (Inc.) "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998.", 3.

<sup>37</sup> GATT Watchdog, above n10, 2.

<sup>38</sup> New Zealand Security Intelligence Service Amendment Bill (No. 2) 1999, no 264-1, explanatory note. [1999 Bill]



There is a change to the definition of security - clause 2(2). The first component (a) "protection of New Zealand from acts of espionage, sabotage, terrorism, and subversion" remains unchanged from the principal Act. Paragraph (b) is new, and is narrower than the existing definition from the 1996 amendment. It provides for "the identification of foreign, or foreign-influenced, capabilities, intentions, or activities within or relating to New Zealand that impact on New Zealand's international well-being or economic well-being."

Clause 3 introduces section 4AA to 'ensure' the political neutrality of the SIS. It requires the Director to ensure that SIS activities are limited to its functions, the SIS is kept free from irrelevant considerations and that the SIS does not further the interests of any political party. Also the Minister is prohibited from directing the SIS to put anyone under surveillance.

## ***B Submissions Addressed in the Second Bill***

### ***1. Security definition***

The security definition, as amended in 1996, was very wide and open to subjective interpretation. By using the phrase 'contribution' to New Zealand's economic or international well-being, it seemed to be authorising surveillance of anyone speaking out against current policies of the government of the day. The 1996 amendment seemed to serve no real, useful purpose. If Parliament had in mind any "...specific activities not already covered by sabotage, espionage, terrorism or subversion, but which greatly threaten New Zealand's interests they should be precisely identified, not covered with a blanket phrase open to widely different political interpretations."<sup>39</sup>

Even with the amended definition it is questionable whether anything is added. Surely "sabotage, espionage, terrorism or subversion", as set out in part (a) of the definition, is a wide enough mandate to cover all those activities the SIS should be concerned with. They would seem to keep the SIS focussed on its prime objective - to ensure the continued existence of a democratic state in New Zealand. Why then does part (b) of the definition include the "identification of foreign .. activities .. that impact on New Zealand's international .. or economic well-being." Does this mean that it is now permissible for New Zealanders to speak out against current government policies, but not someone who is not a New Zealand resident or citizen without coming under SIS scrutiny? Surely if a foreign person, organisation or power is seriously threatening the existence of our democratic state then they would be identified in the process of gathering information to protect New Zealand under part (a). Part (b) therefore appears redundant with respect to the primary focus of the SIS and raises questions as to the validity of and reasons for identifying, and collecting information on, foreign activities if they will not result in any kind of attempted threat to New Zealand society.

### ***2. Joint issuing of warrants***

The argument for Ministerial warrants runs along these lines; the issue of warrants for

<sup>39</sup> The Pacific Institute of Resource Management "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998.", 2.



security reasons is essentially an executive act which the courts should not interfere with. The ongoing dialogue the Minister has with the SIS means that s/he is well placed to assess the value of the information sought as well as the context of the application. Also the issues that need to be weighed in a security case are different to those in a criminal situation. Interception warrants are not comparable to police warrants because they are not used for any criminal prosecution purpose but are simply a means for gathering intelligence. Using judges may also compromise security. The fewer people who know about the detail of warrants issued the more secure an operation is. Since there are a lot of judges sitting at different times, even within a particular court, there is the possibility of many people knowing about an operation should different judges be available when several warrants are sought on the same case. Also differing subjective opinions of judges may lead to inconsistencies as to when warrants will be issued.

On the other hand, it is often argued that an interception warrant should be a judicial one because it appears to offer better external accountability and reassurance that an individual's rights will be protected. Also, although Judges naturally have their biases, their independence from the political process puts them in a much better position to make an objective judgment based on the merits of a particular application rather than being improperly motivated.

The third prevalent view is that the process should be a mixed one. The Minister should naturally be involved in the process since s/he has important experience in political and security matters. However, bringing in a judicial aspect as well implicitly recognises that sometimes someone experienced in the law will see compelling objections to justify the rejection of a request for a warrant.<sup>40</sup>

The creation of the office of Commissioner addresses all of the points raised above. The Minister is still involved in this so called executive act but there is also a judicial element, hopefully affording more protection for the public. The security argument is addressed by not providing for any judge's approval in order to issue a warrant but for the Commissioner's approval, who brings to the position a background in the High Court.

## **VI OTHER ISSUES ARISING FROM THE BILL**

### **A No Need for a Secret Service**

Many submissions were made to the Committee that the SIS is superfluous now that the cold war has ended. Many felt that the SIS has similar objectives to the police and that its functions could be carried out efficiently, and perhaps more effectively, by the police. As was pointed out in one particular submission, "...covert activities do not necessarily require a covert organisation."<sup>41</sup> However it is also important to recognise that in the

<sup>40</sup> Dennis Rose "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998.", 5.

<sup>41</sup> Don Carson "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998.", 1.



current climate of globalisation and increased levels of technology, New Zealand is no longer the isolated little country that we used to be. International terrorists are very well organised and have agents all over the world. No one would wish to see New Zealand become a safe haven for these terrorists, so it probably can be assumed that the existence of the SIS can be justified. Also we have entered into alliances with other countries allowing us to obtain information from their intelligence agencies, and we therefore have a reciprocal obligation to share credible and useful information.

### **B No Accountability**

The Intelligence and Security Committee that oversees the actions of the SIS, and heard submissions for the proposed Bill, is a Prime Ministerial Committee as opposed to a select committee. It is questionable whether this is adequate, especially its two party composition, in light of the proportional representation system. The Committee is made up of very busy people which, when combined with the inability to question secret advice, means the Committee is incapable of providing effective oversight. A select committee on the other hand is theoretically made up of MPs who specialise in a particular area and are more prepared to probe into issues which the agency may prefer to keep to itself.<sup>42</sup> It is, of course, questionable whether this would hold true in practice.

The role of the Inspector-General is one of the statutory checks currently in place. Whether the Inspector-General provided any check on the SIS in the Choudry situation is doubtful given that he was refusing to confirm or deny that the SIS were even involved in the break-in. It is also worth noting that the powers the Inspector General has are investigatory only, so he has no power to give redress for any grievances other than making recommendations to the Prime Minister. Also the Director of the SIS and the Prime Minister may censor the report of the Inspector-General.<sup>43</sup>

The Minister's reports to Parliament, as required by section 4A(5), are no real safeguard. As noted by the Privacy Commissioner "[t]he reports invariably run to three paragraphs. The wording has remained almost identical in the 21 years of reporting .. A formulaic approach has been followed which appears designed to offer ritual reassurance but convey minimal information."<sup>44</sup>

To allow for proper accountability of the SIS a complainant should be allowed to know the defence the SIS is claiming in relation to their complaint, and they should be given the opportunity to refute this defence by way of legal submissions and cross-examination.<sup>45</sup>

<sup>42</sup> Nicky Hager "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998.", 2.

<sup>43</sup> New Zealand Trade Union Federation "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998.", 4.

<sup>44</sup> Privacy Commissioner "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998.", 4.

<sup>45</sup> Democratic Rights Defence Fund "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998.", 4.



There should be provision for people subject to a search under an interception warrant to contest the invasion in open court. However this true accountability is not possible because it is provided in section 4A(6)(b) that the issue of warrants not be subject to judicial review. An argument may be made that purely domestic security cases can be distinguished from those with international connections, like the second Bill purports to do, and that the former should be subject to judicial review but not the latter.<sup>46</sup>

Even without section 4A(6)(b) it is difficult to see how it could be argued that the courts could review the reasons behind a decision to issue an interception warrant due to the subjective wording of the Act itself, which precludes a court returning to the decision and objectively determining whether it was correct. The classic formulation of the distinction between subjective and objective belief is found in Lord Atkin's dissenting judgment in *Liversidge v Anderson*.<sup>47</sup> The central issue before the House of Lords in that case was whether the "reasonable cause" condition in the statute in question was subjective or objective, that is whether it was sufficient that the Secretary of State thought he had reasonable cause or whether the court could determine, objectively, whether he in fact had reasonable cause. Lord Atkin held that reasonable cause is an objective test.<sup>48</sup> This has been accepted in New Zealand, where it has also been held that "good cause" is not materially different to "reasonable cause."<sup>49</sup>

However, the SIS legislation, both before and after amendment, makes no reference to either "reasonable cause" or "good cause" to believe in relation to the issue of interception warrants. Indeed section 4A(1) says that an interception warrant may be issued "...if the Minister and the Commissioner are both satisfied .. that the conditions specified .. apply." Similarly worded sections, requiring only satisfaction, were referred to by Lord Atkin as being "...plain that unlimited discretion is given.." provided that the Minister acts in good faith.<sup>50</sup> This must necessarily be the case. Were they to be given the same meaning there would be no point in using the different phrases "reasonable" and "satisfied." Therefore, even disregarding the express exclusion of the courts jurisdiction, the only way the Minister's decision could be questioned would be to bring into doubt the Minister's honest belief that the criteria were satisfied.

The inclusion of section 4A(1)(b) removing any right to judicial review, as well as the very wording of the statute, substantially impairs true accountability. The argument may be raised, analogous to the argument in *Choudry* in relation to the discovery application, that showing reasonable grounds for the Minister's decision would impair security by requiring the production of sensitive material. The answer to that is simply that should the Crown refuse to produce evidence proving reasonableness where it is brought into question, the court would not force the production of the alleged sensitive material but would simply enter a finding for the plaintiff on the grounds of no defence raised.

<sup>46</sup> Crowder, above n3, 159.

<sup>47</sup> [1942] AC 206 (HL). [*Liversidge*]

<sup>48</sup> *Liversidge*, above n47, 227-228 per Lord Atkin dissenting.

<sup>49</sup> See *Police v Anderson* [1977] NZLR 233 (CA); *Meates v Attorney-General* (Customs Department) [1981] 2 NZLR 335 (HC); *Dulcie Holdings Ltd v New Zealand Customs Service* [1997] DCR 1077 (DC).

<sup>50</sup> *Liversidge*, above n 47, 233 per Lord Atkin dissenting.



**C     *Search and Seizure Already has Widespread Legislative Provision***

The Summary Proceedings Act, the Misuse of Drugs Act and many others provide for powers of search and seizure. These powers typically require prior approval from an independent authority, except in specific situations. The person whose property is to be entered is entitled to know that it is and pursuant to which authority. Also such entry is generally open to legal review. Given the wide range of circumstances that already exist to justify entry it is questionable whether these circumstances need to be extended, and in such a fashion as to remove all the safeguards and specificity the courts and legislature have introduced over the years.<sup>51</sup>

**D     *Did the 1977 Parliament Intend the SIS to have the power?***

It has been argued by many, including Prime Minister (PM) Rt Hon Jenny Shipley and Opposition Leader Rt Hon Helen Clark, that the Bill in fact gives no new powers to the SIS - that it actually just confirms the powers that it has always been presumed to have.<sup>52</sup> This is evidenced, so the argument goes, by the comments of both the PM at the time, Rt Hon Robert Muldoon, and the then Leader of the Opposition, Rt Hon Bill Rowling. The then PM said, in debate, that "...the possession of an interception warrant might authorise breaking and entering, but it would not absolve the person named in the warrant from committing, for example, a theft."<sup>53</sup> In opposition to the Bill Rt Hon Bill Rowling said "...the interception warrant gives power not only to open mail and tap phones, but also to break into private premises."<sup>54</sup>

However there was no such express recommendation given in the Powles Report, and surely any anticipated intrusion on individuals' rights would have warranted a full discussion in his report. Also there are other statements made by members of the House during the 1977 debates which seem to conflict with the PM's and Opposition Leader's comments. For example, Government MP Barry Brill said "The Bill does not extend the powers of the Prime Minister and the SIS; it restricts the powers."<sup>55</sup> So it would seem that individual comments made by members, especially if not picked up on and contested by other members, are nowhere near conclusive. In the end it all boils down to the fundamental constitutional principle that if Parliament is going to infringe upon fundamental rights of citizens then it needs to do so expressly and clearly. In the 1977 amendment no such express provision for entering onto private property was made and so it cannot be presumed that Parliament intended to do so.

**E     *Breach of the International Covenant on Civil and Political Rights***

*Article 17:* (1) No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks upon his honour and reputation.

<sup>51</sup> Rose, above n40, 2.

<sup>52</sup> (15 December 1998) 574 NZPD 14663.

<sup>53</sup> (8 September 1977) 413 NZPD 2783.

<sup>54</sup> (18 October 1977) 414 NZPD 3722.

<sup>55</sup> (4 November 1977) 415 NZPD 4224.



*Article 19:* (1) Everyone has the right to hold opinions without interference.  
(2) Everyone has the right to freedom of expression..

The Bill increases the level of 'interference' that may be exercised by the SIS. 'Interference' clearly covers intrusion onto property, into communications and the seizing of any communications or documents. These interferences can be classified as arbitrary in that the body carrying out the interferences has no realistic accountability to the public, there is no room for judicial supervision or review in the principal Act, nor is there any sufficient compensation available to complainants. Under the existing Act the argument is even stronger, for the SIS can institute surveillance under the undefined phrase of contributing to New Zealand's economic and international well being. Due to the subjective and imprecise nature of these terms any search on these grounds would necessarily be unpredictable, depending largely on who was defining the terms at the time, and therefore arbitrary.<sup>56</sup>

The *Choudry* case would seem to legitimately raise concerns that the SIS are being used to target political activists who are no real threat to New Zealand security at all. That Mr Choudry's assertions as to the type of activity he was involved in at the time of the search, that is purely political, have never been challenged serves to fuel the speculations. If this is what the service is being used for then this clearly contravenes Article 19, not to mention the principal Act itself.

#### *F Not Many Warrants*

It is argued by some that there is a lot of needless fuss about interception warrants because there are not very many issued during a year, usually about 4 or 5.<sup>57</sup> However the number of warrants issued really misses the point because they can be in force for a long time and can cover many people, places and organisations.

#### *G Lack of Competency Examples*

There are reports of surveillance of Trade Unions, peace movements, the anti-Vietnam war movement, the anti-apartheid movement and refugees who, in the opinions of the intelligence agencies of the regimes they are fleeing, are viewed as dangerous.<sup>58</sup> It has also been rumoured that the SIS at one stage monitored anyone opposed to the sale of SOE's, clearly an example of political use of the SIS if true.<sup>59</sup> In 1986 Ms Wendy Walters, a Public Service Association delegate and parliamentary secretary, went public after the SIS approached her to undertake some political spying.<sup>60</sup> There are many other reports of dubious SIS activities, though more often than not they are unconfirmed which is hardly surprising given the lack of information forthcoming from anyone connected to the SIS. The credibility of the SIS is further undermined when these reports are coupled

<sup>56</sup> New Zealand Trade Union Federation, above n43, 7.

<sup>57</sup> Privacy Commissioner, above n44, appendix.

<sup>58</sup> The Alliance Party, "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998.", 1.

<sup>59</sup> Peace Council of Aotearoa New Zealand Incorporated, "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998.", 3.

<sup>60</sup> Spy-Catching Rebounds in Caucus" *The Dominion*, Wellington, New Zealand, 10 Nov 1986, 2.



with the perceived failures of the SIS, such as the Rainbow Warrior bombing where the popular understanding is that the police brought the French people involved to justice not the SIS, the loss of apple cuttings to Chilean orchardists, not to mention that the *Choudry* case seems to illustrate that "...the SIS can't even pull off a routine covert break-in without being caught and traced."<sup>61</sup>

#### *H Is it Possible for the SIS to Act Properly Without the Power?*

It is argued that without a power of covert entry onto premises the SIS would not be able to effectively carry out its functions. However, there are strong arguments to suggest that this power is not necessary at all. As GATT Watchdog commented "...technology [has] advanced far enough to mean that listening devices do not need to be placed inside telephones or under picture frames as in Bond movies..."<sup>62</sup> There has been a dramatic increase in the types of communications as well as the ways in which interception can be implemented. All of these fall within the ambit of the 1977 provision, making it an untenable position to claim that the SIS cannot perform its functions without a power to enter private property.

#### *I Bill of Rights Act 1990, Section 21*

It is arguable that the interception warrant scheme allowing for entry onto personal property is contrary to section 21 of the BORA, protecting against unreasonable search and seizure. Arguably the scheme is unreasonable due to the factors discussed above in relation to arbitrariness, that is citizens are not informed that they are having their houses searched and why, they have no realistic recourse to the Courts to review the powers exercised, the current definition of security means the grounds on which warrants can be issued are vague and open to subjective interpretation leading to unpredictable application and what control mechanisms there are are widely perceived as inadequate.

However, the flipside to this argument is that any inconsistency with the BORA does not have to be remedied by reading in requirements more consistent with the BORA, as the Courts have been willing to do in the past.<sup>63</sup> This is because section 5 of the BORA allows for infringements of the BORA rights provided that they are "...demonstrably justified in a free and democratic society." Arguably the powers in the Bill are demonstrably justified in that they are designed to protect New Zealand from terrorism and espionage ensuring that we remain a democratic society. For those that view the SIS as acting on behalf of the Government with a political agenda and targeting those with opinions that differ from the majority, then clearly the powers are not demonstrably justified and in fact run contrary to democracy, which has at its heart the voicing of political dissent.

<sup>61</sup> Anti-Bases Campaign "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998.", 1.

<sup>62</sup> GATT Watchdog, above n10, 2.

<sup>63</sup> See for example *R v Laugalis* (1993) 1 HRNZ 466 (CA).



## VII CONCLUSION

Attempting to balance notions of security with public accountability is something New Zealand has always struggled to deal with, and always will due to its irreconcilable nature.

However, in 1969 New Zealand probably chose the most democratic way of dealing with this conflict when Parliament drew the SIS out from the shadows of Crown prerogative and created a statutory body.

The wheels of change in a democracy have never been anything but lumbering, and recent events relating to the SIS have borne that out. However, despite the 30 year wait since the SIS became a statutory body, these events have also provided an adroit illustration of how the democratic process of checks and balances is supposed to work. In 1996, when Parliament wanted to change the definition of security, it had to do so publicly and concurrently increase the accountability provisions. Soon after the *Choudry* case provided the courts with an unusual chance to peruse the 1977 Amendment, and to ultimately hold that the legislation did not allow for covert entry into private premises. Following on from this, in 1998/1999, Parliament has had to clarify and specify what the powers of the SIS are. Again it had to do so publicly, and respond to public demands for more accountability through the increased specificity of all areas relating to the SIS, and the creation of the Commissioner's role.

As the century draws to a close so does this latest chapter of New Zealand's attempts to fit the SIS within a democratic, open government framework. It is clear that the struggle between accountability and security will continue well into the future. What is not so clear is the full impact of the recent changes to the principal Act and, if history is anything to go by, that information will not be available for several years yet.



**BIBLIOGRAPHY**

Anti-Bases Campaign "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998."

Association of University of New Zealand (Inc.) "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998."

Auckland Council for Civil Liberties "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998."

Australian Security Intelligence Organisation Act 1979

Canadian Security Intelligence Act 1984

*Choudry v Attorney-General* (19 August 1998) unreported, High Court, Christchurch Registry, CP 15/98.

*Choudry v Attorney-General* (9 December 1998) unreported, Court of Appeal, CA217/98.

*Choudry v Attorney-General* (6 July 1999) unreported, Court of Appeal, CA 217/99.

*Corbett v Social Security Commission* [1962] NZLR 878 (CA).

Court of Appeal Rules in Favour of SIS" *Salient*, Wellington, New Zealand, 12 July 1999, 9.

Democratic Rights Defence Fund "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998."

Dennis Rose "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998."

Don Carson "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998."

*Dulcie Holdings Ltd v New Zealand Customs Service* [1997] DCR 1077 (DC).

Dunedin Community Law Centre "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998."

*Entick v Carrington* (1765) 95 ER 807 (KB).

G. Crowder "The Security Intelligence Service Amendment Act 1977 and the State Power to Intercept Communications" (1977/78) 9 VUWLR 145.



GATT Watchdog "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998."

H.P Lee, "The Australian Security Intelligence Organisation - New Mechanisms for Accountability" (1989) 38 ICLQ 890.

*Haj-Ismail v Maddigan* (1982) 45 ALR 379 (FCA).

Ian J Lloyd "The Interception of Communications Act 1985" (1986) 49 MLR 86.

Ian Leigh and Laurence Lustgarten. "The Security Services Act 1989" (1989) 52 MLR 801.

Intelligence Services Act 1994.

John Wadham, "The Intelligence Services Act 1994" (1994) 57 MLR 916.

L.L.I.J Edwards "The Canadian Security Intelligence Act 1984 - a Canadian Appraisal" (1985) 5 Oxford J Leg Studies 143.

Lawrence Lustgarten "Accountability of Security Services in Western Democracies" (1992) 45 Current Legal Prob 146.

*Liversidge v Anderson* [1942] AC 206 (HL).

*Meates v Attorney-General (Customs Department)* [1981] 2 NZLR 335 (HC).

*Morris v Beardmore* [1981] AC 446, 464 (HL).

New Zealand Council for Civil Liberties, Report on the New Zealand Security Service Intelligence Act 1969, (Wellington, 1971).

New Zealand Security Intelligence Service Act 1969.

New Zealand Security Intelligence Service Amendment Act 1977.

New Zealand Security Intelligence Service Amendment Act 1996.

New Zealand Security Intelligence Service Amendment Bill 1998, no 259-1.

New Zealand Security Intelligence Service Amendment Bill (No. 2) 1999, no 264-1.

New Zealand Trade Union Federation "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998."



Nicky Hager *Secret Power: New Zealand's Role in the International Spy Network* (Craig Potton Publishing, Nelson, 1996).

Nicky Hager "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998."

Peace Council of Aotearoa New Zealand Incorporated, "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998."

Philip Leach, "The Security Service Bill" (1996) 146 New L J 224.

*Police v Anderson* [1977] NZLR 233 (CA).

Privacy Commissioner "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998."

*R v Laugalis* (1993) 1 HRNZ 466 (CA).

Report by Chief Ombudsman Security Intelligence Service (Wellington, 1976).

Security Services Act 1989.

Sir Geoffrey Palmer "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998."

Spy-Catching Rebounds in Caucus" *The Dominion*, Wellington, New Zealand, 10 Nov 1986, 2.

The Alliance Party, "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998."

The Pacific Institute of Resource Management "Submission to the Intelligence and Security Committee on the New Zealand Security Intelligence Service Amendment Bill 1998."

United Kingdom Interception of Communications Act 1985.



e  
AS741  
VUW  
A66  
B275  
1999

<b>LAW LIBRARY</b> A Fine According to Library Regulations is charged on Overdue Books.		<b>VICTORIA UNIVERSITY OF WELLINGTON  LIBRARY</b>
<del>15/6/00</del> 19/12/2000 19. DEC. 2000 <b>20 NOV 2003</b> 8pm		

VICTORIA UNIVERSITY OF WELLINGTON LIBRARY



3 7212 00608804 9



e  
AS741  
VUW  
A66  
B275  
1999



